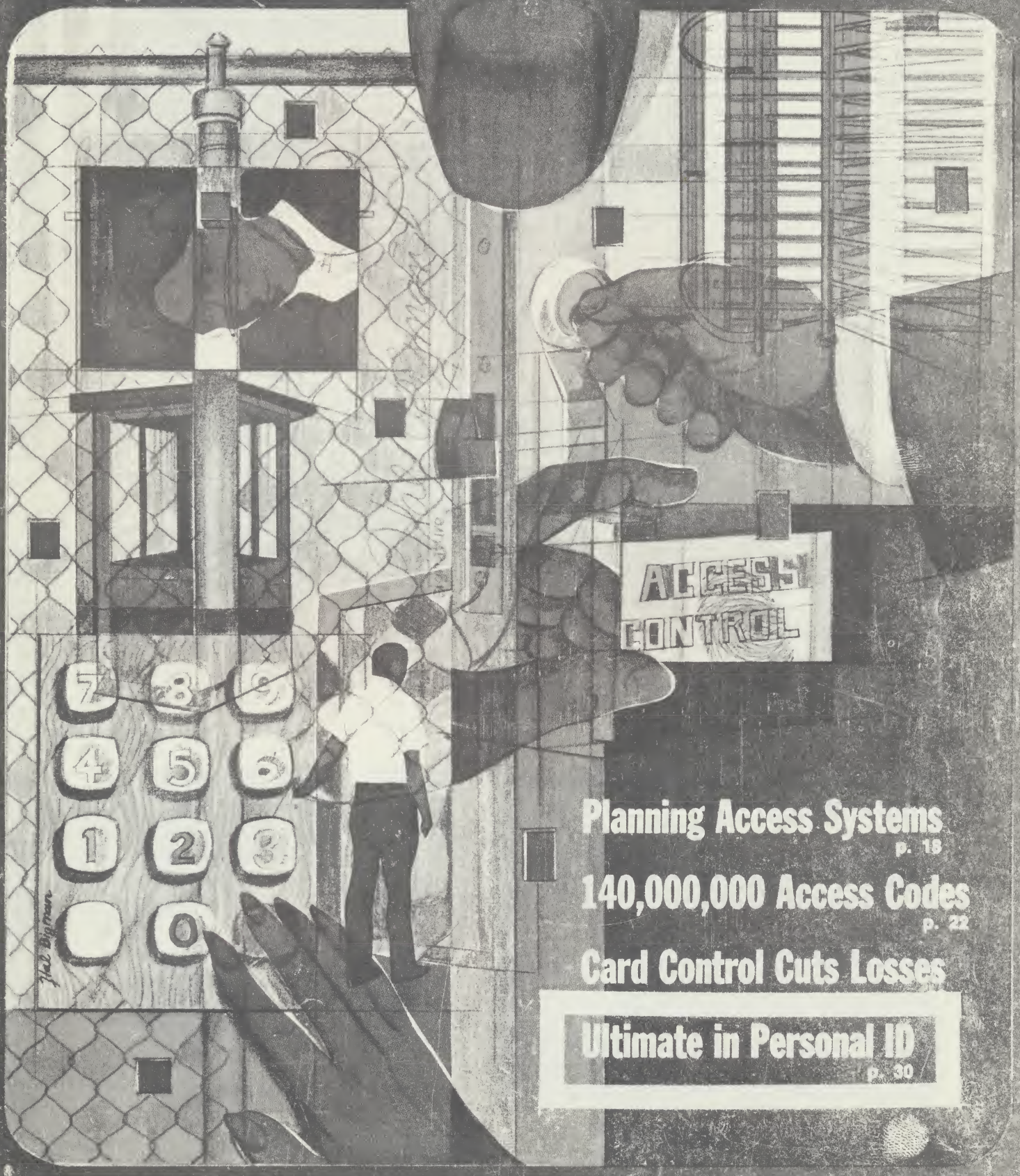
SEPTEMBER, 1975/Volume 12, Number 8

Security World

THE MAGAZINE OF PROFESSIONAL SECURITY ADMINISTRATION AND PRACTICE



Ultimate Security in

Fulfilling of space-age demands may lead to guaranteed security and reliability by ID use of non-reproducible physical characteristic . . . clearly tamperproof AND detectable by machine.

There are three ways in which a person can be identified by an automated system:

1. By something he knows or remembers (an ID number or password).
2. By something he carries (a badge, key, key-card, *etc.* that will activate a device at the access point —where the item is recognized).
3. By a device that can use some physical measurement of the person. (These devices can measure static characteristics such as height, weight, hand dimensions, or fingerprints; or may use dynamic characteristics such as voiceprint or handwriting.)

The greatest reliability is, of course, attached to the use of characteristics unique to the person to be identified. A signature verification instrument has recently been developed that meets military specifications for accuracy. Such verifications of individual characteristics add new dimensions to the security tasks of personal identification and access control.

Since the signature system is now being marketed, security managers have had the opportunity to raise their many questions. Among these are: How does it work? Who will use it? Does it establish a high enough standard of personal identification? Can it be interfaced with other security/access control systems? How can it be used? How does it hold up in everyday use (*i.e.*, too expensive, too unreliable, too delicate to operate)?

Certainly such answers must be individual to the particular situations and circumstances faced by each security manager. As with any security system, managers must weigh the value of the assets to be protected against the cost of such a system, and also realize that automated identification systems are a complement to (not a replacement for!) such established security measures as competent guards, secure facilities, and other protective devices.

To approach the answers to these questions, the principles behind the system recently developed will be discussed along with future use and market considerations.

HOW DOES IT WORK?

The basic technology behind the signature verification equipment is fairly straightforward. It relies upon five established facts:

1. A person's signature is one of the most consistent and automatic activities of his life.
2. Certain aspects of a signature are unique to each individual.
3. People are accustomed to signing their names as a means of identification.
4. The process does not require learning or memorization.
5. A signature is relatively stable over time, and any changes that occur are gradual.

The basic task was to determine *what* to measure in a signature, and how to measure it *effectively*.

It was determined that the most effective point of measurement was the pressure applied by a pen on paper. The pressure pattern is unique to the individual, yet remarkably constant from one signature to the next.

A pen was therefore developed that converted the varying pressures during a signature to an electrical signal.

Figure 1 shows what would result if the signal generated by the pen pressure were plugged into a chart recorder.

The capabilities of computers allow the pen pressure to be measured discretely many times a second—well beyond any conceivable ability of the human eye to perceive. Yet the pressure pattern of a signature is only indirectly related to its appearance, so it is impossible to determine the pressure pattern of a signature by the "looks" of it—thus preventing the pressure from being forged as well as eliminating eye examinations as a means of detecting forgeries if pressure is used as a criterion. Graphic analysis of the signature was avoided because of the relative ease of forging the graphical representations and the relative accessibility of forgers who have signature samples with which to practice.

In operation, a person to be enrolled in a signature verification system signs his name with the special pen three to six times to establish his personal "signature standard." Then, when he wishes to verify his identity

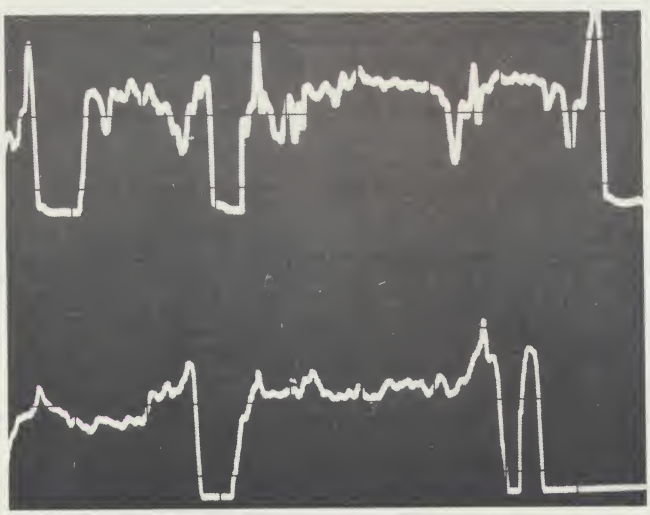


Figure 1. Actual vs forged signature can be determined by oscilloscope tracing. Above: top line is oscilloscope tracing of pattern of pressure on valid signature; bottom line is tracing of attempted forgery. Clearly dissimilar, the forgery was denied access.

Figure 2. Individual in photo above is writing his name for verification. His pen pressure creates an individualized characteristic that identifies him as signator. It is then automatically compared with his signature file in the microcomputer.

Personal Identification?

by Jim Davis

on the system (*e.g.*, in order to gain access to a restricted area), he merely makes a claim on the system through a codeword entered on a console, or by inserting a card into a card reader, and signs his name with the special pen. The computer then compares the pressure pattern of the signature with the signature standard stored in its memory. If it matches, access is granted.

Using the dynamic measurements of pressure and time makes forgery extremely difficult since it hides the form of input (the human eye cannot monitor the pressure applied in time), and the *security* of such an access system therefore approaches infinity. But does a person sign his name the same way every time, or to phrase it another way, will the system display low reliability by rejecting rightful claimants?

The answer to the first question is yes—within adjustable statistical limits and unless the claimant is suffering from a neurological disorder. Over time, however, a person's signature does change very gradually. With the computer, however, the security equipment can accommodate this fact by refining an individual's signature standard every time he successfully verifies his identity.

The answer to the second question, which concerns rejecting rightful claimants (*i.e.*, reliability), depends upon the degree of security desired. The functional limits of the system can be loosened or tightened, and rejecting rightful claimants is, after all, mostly a nuisance factor.

For the most part, a claimant is allowed three chances to establish his identity. With this standard, the system will reject less than 1% of rightful claimants on the first attempt.

Some people (among the 1 % of those refused access) present problems to the system because of highly unstable signatures. By minimal training, adjustment of tolerances, or substitution of an alternative verification scheme (or algorithm), these individuals also can be brought within the scope of the system.

The capability for tightly adjusting the tolerances of the system, it should be noted, is important to the system user. When tolerance limits are tight, access will be refused to those under excessive alcoholic or emotional stress —on the same basis that the system would deny neurological disorders. Since this can be done either for specified individuals in the system, or across the whole system, off-hours access by employees with temporary difficulties or other problems, can be dealt with securely and discreetly. This capability could be particularly important for diplomats or other government figures who have access to national secrets, or for corporate executives in foreign countries, any of whom may be liable to terrorist activities (*e.g.*, kidnaping of families) in order to force them to furnish access to unauthorized persons. In such a case, of course, the system would detect the stress from the pen pressure reading. Access would not necessarily be refused; but rather, the system could relay a signal to a remote security officer.

The central console consists basically of a microprocessor, a keyboard, and a printer. It performs the same tasks as in many card-reading access control systems—printing a record of claims accepted and rejected at each station, enrolling new members, locking out members no longer authorized for entry, *etc.*

The access stations consist of a special pen and a device to call up the central console's microprocessor—typically a card reader or keyboard—and also other associated devices such as electro-magnetic locks. A user who already has excess computer capabilities could have the software installed in his own computer, and let it control access.

Users who are involved in special situations may want the chances for subversion to be, for example, less than 1 in 500,000. In that case, a number of separate algorithms (the rules by which the verifying computer program compares signatures) can be installed in the controlling computer.

In instances where material or information of incalculable worth is to be protected, and where only a dozen or so persons would have access, it is conceivable that a user may want a separate algorithm for *each* individual, with very tight tolerances on each.

APPLICATIONS

Commercial firms could use the system to control access to highly sensitive areas and materials. Let us take the example of a national financial firm with a central data processing facility that can be accessed from remote branches. For such a firm, computer misuse could obviously substantially damage its business, and computer sabotage could destroy it. A signature verification system could be installed at its central computer facility, so that the transmission of signature data would be accomplished using the same communications lines as the terminals for access. In this way, access would be controlled on any properly equipped terminal to (1) the computer resources as a whole or (2) any individual resource such as a file or data base.

Another commercial use lies in the future. A person's signature standard consists of computer data. This data can be transcripted onto the magnetic strip on such items as credit cards, bank identification cards, *etc.* The identity of someone using such a card could then be verified by a small, independent desk-top device.

This stand-alone device would, basically, read the data on the card and compare it with the data generated by the person's signature. The very gradual change in a person's signature is an added advantage to the card issuer, since such cards are generally issued for a one to three year period of time. Preliminary findings show frequency of "retardation" to be well above one year for the vast majority of people—a convenient automatic check point.

The same concept can also be used by law enforcement agencies. It has been found that, not only does a person sign his name with remarkable consistency, but he also forms characters in writing with consistency. A standard could therefore be formulated on the way a person signs only his initials, writes a word or a combination of words, draws a specified symbol, *etc.*

SUMMARY

The signature identification system is based upon a relatively simple concept made feasible by sophisticated use of computer technology. What it measures in a signature is impossible to determine by the signature's appearance and virtually impossible to duplicate because of the speed of measurement, the amount of data obtained, and the thousands of comparisons made with each bit of data. It represents a flexible working system for automated protection of high-security areas and is a distinct contender as a potential for everyday access control use in the future.

James K. Davis

James K. Davis is currently systems consultant to Damon Corporation for positive identification systems. Formerly Executive Vice President of Fire Controls Inc. of New York City, he directed the development of one of the first card reading access control systems and the development of life safety fire communications systems. Previously, he was head of the fire protection department of Meyer, Strong, and Jones, consulting engineers. He also consulted on security and fire protection to many major corporations, including American Tobacco Company, Bankers Trust Company, and Equitable Life Insurance Company. As a designer for Vitro Engineering Company, he directed the design of fire protection systems for such sites as nuclear power plants and military installations. He attended Brooklyn College and the City College of New York.

The Signac™ Signature Access Control System is marketed by Damon Corporation. Contact James K. Davis at (212) 689-2885 for further information.